Maleficent Lightning Rods for Non-Attributable Physical Attacks on Electrical Infrastructure Using Low Cost Approach

15 April 2024
Simon Edwards
Research Acceleration Initiative

Introduction

Although a great deal of precautions have been taken against cyberattacks against utility infrastructure, direct physical attacks are far more devastating, take longer to repair and are more expensive to repair. While some forms of physical attack (as in the case of a string of incidents in 2022 in which bullets were fired at electrical substations) would never be mistakenly attributed to an accident, novel technologies combined with low-tech approaches make it possible for utility equipment sc. electrical substations to be targeted in such as way so that these events could be misattributed to chance weather-related effects.

Abstract

Harnessing the natural power of lighting, which when it strikes sensitive infrastructure per chance can cause non-trivial damage, has the potential to enable two distinct implementation scenarios: One, a passive, low-intensity attack in which a handful of targets are struck over a period of months and the other, an aggressive coordinated regional assault which could result in a weeks-long outage over an area spanning multiple States.

The mode of such a potential attack would involve drones equipped with ultra-thin (to keep weight low) metal wire similar to that used in wire-guided missile systems such as the TOW. Pairs of tandem drones could be flown to points directly above electrical substations just prior to the arrival of intense lightning. The wire would run from the bottom of Drone A into a port in the top of Drone B, which would need to leave enough space for the wire to pass between the rotors of the drone without risking getting tangled in the rotors. This could be prevented using a wire guide which runs through the space between the rotors of Drone B and extends for a distance above the rotors. Drone B would remain about 50 feet above a targeted substation and would hold position, bracing its end of the wire to ensure that any attracted lightning directly strikes the substation. Drone B would loiter at a sufficiently high altitude so as not to enter the field of view of surveillance camera, but not at such a high altitude that lightning would be significantly likely to divert in some other direction after being guided by the overall mechanism for the majority of the journey from the cloud to the ground. The drones used would need to be capable of algorithmic flight stabilization in high wind conditions and capable of remaining aloft for 10-15 minutes carrying a heavy spool of wire.

The drones, coupled with the wires, would act as lightning rods designed to, rather than ensure that lightning is diverted away from a structure in order to protect the structure as with a traditional lightning rod, would instead ensure that the structure is hit directly by dangling a thin lightning rod which extends all the way from the cloud level to about 50 feet AGL and which, as it would not be grounded, would merely act as a guide for the lightning until it reached Drone B, at which point it would continue to move without guidance toward the ground and toward the intended target.

Conclusion

Such an attack would all but guarantee the destruction of millions of dollars worth of electrical equipment in each sortie and would leave little physical evidence as there is no reason for the drones pass in front of surveillance cameras (they can be launched from some distance away) and as the lightning would incinerate nearly all drone remnants. What fragments would remain would likely be blown by the wind to outside of the perimeter of the secure area associated with the substation or would be mistaken for substation components or other sundry debris.

If one didn't care about the possibility of foul play being suspected, a coordinated attack against multiple targets on a regional scale could be implemented by a few dozen teams in a particular area expecting to experience intense lightning at a given time.

It is remarkable that some malicious entity has not, as of yet, attempted such an attack, which could be used not only to target substations, but literally any transformer or exposed wire. It may, alternatively, be used to start wildfires or structural fires.